PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

Intyg
Certificate

15

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71) *Sökande* / *Applicant (s)* — *Telefonaktiebolaget L M Ericsson, Stockholm SE*

(21) *Patentansökningsnummer* / *Patent application number* — *0202450-3*

(86) *Ingivningsdatum* / *Date of filing* — *2002-08-15*

Stockholm, 2003-04-30

För Patent- och registreringsverket
For the Patent- and Registration Office

Lina Oljeqvist

Lina Oljeqvist

Avgift
Fee

PATENT- OCH REGISTRERINGSVERKET
SWEDEN

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

NON-REPUDIATION OF DIGITAL CONTENT

TECHNICAL FIELD

The present invention generally relates to digital rights management (DRM) for managing digital content provided over networks, and more particular to methods, equipment and systems used for monitoring usage of digital content by a client in a DRM system.

BACKGROUND

The distribution of digital content or media data using modern digital communication technologies is constantly growing, increasingly replacing the more traditional distribution methods. In particular, there is an increasing trend of downloading or streaming digital content from a content provider to a client or user, which then typically renders the content using a rendering device according to some user rights, or usage rules specified in a license associated with the digital content. Due to the advantages of this form of content distribution, including being inexpensive, fast and easy to perform, applications can now be found for distribution of all types of media such as audio, video, images, electronic books and software.

However, with this new way of distributing digital media content comes the need for protecting the content provider's digital assets against unauthorized usage and illegal copying. Copyright holders and creators of digital content naturally have a strong economic interest of protecting their rights, and this has lead to an increasing demand for digital rights management (DRM). DRM is generally a technology for protecting the content provider's assets in a digital content distribution system, including protecting, monitoring and restricting the usage of the digital content as well as handling payment. A DRM system thus normally includes components for encryption, authentication, key management, usage rule management and charging.

The most basic threats to a DRM system include eavesdropping, illegal copying, modification of usage rules, and repudiation of order or delivery of content. Most of these basic security problems are solved by standard cryptographic techniques, including encryption, authentication and key management. However, what basically distinguishes the security problems of a DRM system from other general security problems is that not even the other end-part of the communication (the user) is completely trusted. In fact, the end-user might want to try to fraudulently extend his usage rights, for example rendering the media content more times than he has paid for or illegally copying the digital content to another rendering device. Therefore, some form of rule-enforcement is required in the client's rendering device. To this end, a DRM agent implemented as tamper-resistant circuit in the rendering device and some formal language expressing the usage rules are commonly used together with the basic cryptographic techniques mentioned above.

However, while the DRM agent (at least theoretically) enforces the usage rules and keeps the usage according to the license, it per se does not guarantee that the client will not repudiate the usage of the digital content. For example, the client may have paid to watch a downloaded movie three times, but claims that due to some malfunctions he was only able to watch it twice. The client then disagrees with the DRM agent in the rendering device about the number of renderings he has consumed. This can easily escalate into a legal process, especially if it regards a high valued digital content, for which the client has paid a large sum of money for the usage rights.

The prior art DRM systems and rendering devices incorporating DRM agents do not provide any mechanisms to minimize the risk of disagreement between the client and DRM agent, discussed above, or in the case it has happened, any mechanisms to support the defense of the DRM agent and thereby support the defense of the device manufacturer and the DRM system manufacturer.

SUMMARY

The present invention overcomes these and other drawbacks of the prior art arrangements.

It is a general object of the present invention to provide a digital content usage monitoring functionality in a DRM system.

It is another object of the invention to provide methods, equipment and systems for deterring clients from repudiating usage of digital content received from a content provider of a network.

Yet another object of the invention is to provide a client module incorporating a logging agent for logging information of usage of received digital content.

A further object of the invention is to provide methods and systems for effectively and flexibly downloading and implementing logging agents in client modules.

These and other objects are met by the invention as defined by the accompanying patent claims.

Briefly, the present invention involves arranging or implementing a logging agent in a client module used for using digital content ordered and received from a content provider of a network, e.g. Internet or a wireless network for mobile communication. This logging agent monitors the usage of the content, performed by the client, by logging information concerning the usage individually for each usage to be monitored. The generated usage information is then stored as a log entry in a dedicated log, either arranged in the client module or provided externally by a trusted party, e.g. a network operator or the content provider.

The usage performable by the client includes rendering or playing, saving, forwarding, copying, executing and/or modifying the digital content. Usage rights or rules of the relevant methods of client-usage to be monitored are preferably specified in a license associated with the digital content.

By logging or recording information of client usage, the logging agent according to the invention has a repudiation deterring effect on clients, lowering the risk that clients violate usage rules of ordered digital content. The generated usage log can also be used if a disagreement between the client and the content provider (through a DRM agent implemented in the client module for enforcing usage according to the usage rules) is present. By simply investigating the log, information about the actual number of usages performed by the client, when they were performed, the usage quality obtained during the rendering session (depending on what is included in the usage information) can be retrieved and used to solve any issues.

The usage information includes elements, which concern the actual usage of the digital content. The elements may comprise a representation of the digital content, e.g. the associated file name or a fingerprint of the content, including the content itself or a hash function thereof. In addition, information of usage quality may be included, e.g. specifying the bandwidth and/or resolution of the content and/or the obtained sample rate if the content is delivered as streaming data. The usage time of the content is preferably also found in the information. The usage information may also be authenticated, e.g. by an authentication tag, digital signature, message authentication, identifying from which client the information is derived.

The logging agent is preferably implemented in software, hardware or a combination thereof in a DRM agent of the client module, or in connection with a rendering device associated with the module, and performs the actual rendering of the digital content. In order to prevent an attacker from illegally accessing and modifying the generated usage information, the information is preferably cryptographically protected using an

encryption key. The associated decryption key can then be stored at a trusted party.

The security of the logging agent is also increased by implementing it in a tamper-resistant device, which preferably is removably arranged in the client module for allowing the device, including the logging agent, to be moved between different client modules. A preferred tamper-resistant module is a network subscription identity module issued by the network operator, e.g. standard SIM cards used in GSM (Global System for Mobile Communications) mobile telephones but also UMTS (Universal Mobile Telecommunications System) SIM (USIM), WIM (Wireless Identity Module) and ISIM (Internet Multimedia Services Identity Module) cards can be used. When implemented on a SIM, the logging agent can use the authentication and cryptographic functions of the SIM for use on the usage information. In addition, keys associated with the SIM subscription can be used for performing usage information authentication and encryption.

The logging agent is preferably implemented in an application environment provided by an application toolkit associated with the SIM, e.g. SIM Application Toolkit (SAT) or UMTS SAT (USAT). The SIM may be pre-manufactured with the logging agent or the logging agent may be securely (preferably authenticated and encrypted) downloaded from a network operator associated with the SIM. Commands associated with the SIM – client module interface are used for downloading and implement the logging agent in the application environment. The same commands can also be used for subsequently receive and implement upgrades of the logging agent.

The logging agent according to the present invention may be arranged in any client module adapted for receiving digital content of a network, including personal computers, mobile units, e.g. mobile telephones, personal digital assistants or communicators.

The invention offers the following advantages:

- Provides strengthened defense for equipment manufacturer, network operator and content provider in a situation where a dispute is present, on whether usage of digital content by a client module actually has been performed or not.
- Deters clients from repudiating usage of the digital content according to usage rules associated with the content or by trying to violate the rules.
- From the end-user point of view, the invention provides flexible and upgradable implementation of logging agents, as well as "portability" between different client modules.
- A network operator can efficiently manage and upgrade logging agents connected to the network, and the invention also opens up new business possibilities for the operator acting as a trusted center for content distribution.
- Provides useful information of usage of digital content, performed by clients, which information can be used by content providers when deciding business models.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention together with further objects and advantages thereof, may best be understood by making reference to the following description taken together with the accompanying drawings, in which:

Fig. 1 is an overview of a digital content ordering and distribution system incorporating the relevant parties and their mutual relationships;

Fig. 2 schematically illustrates an embodiment of a client module according to the present invention;

Fig. 3 schematically illustrates another embodiment of a client module according to the present invention;

Fig. 4 is an illustration of a logging agent according to the present invention with cryptographic and authentication functionality;

Fig. 5 is an overview of a log storing log entries with usage information of client-usage of digital content;

Fig. 6 schematically illustrates yet another embodiment of a client module according to the present invention;

Fig. 7 illustrate a tamper-resistant device comprising a logging agent according to the present invention;

Fig. 8 is a flow diagram illustrating the steps of a monitoring method according to the present invention;

Figs. 9A-9B illustrate flow diagrams of embodiments performing one of the steps in Fig. 8; and

Fig. 10 is a flow diagram illustrating the steps of a digital rights management method according to the present invention.

DETAILED DESCRIPTION

The present invention is generally applicable to digital rights management (DRM) used in a digital content ordering and distribution system. In such an ordering and distribution system, digital content or media is provided from a content provider to a client over a network, e.g. Internet or a wireless network for mobile communication, managed by a network operator. In order to facilitate understanding of the invention, a brief discussion of the general functionalities of DRM follows. As was mentioned in the background section, DRM is used for protecting the copyright holders' assets in a digital content ordering and distribution system. In this system, DRM typically regards authentication and key management, usage rights management and charging. These DRM functionalities are implemented in DRM modules arranged in the relevant parties, i.e. for example in a client module, in a server of the network operator and in a media or content server of the content provider.

Starting with authentication and key management, authentication is used to identify the parties in the digital content ordering and distribution process. Techniques well known in

the art, such as message authentication and digital signatures using cryptographic keys [1], may be employed for authentication. In addition, techniques for marking or stamping digital content so that it can be tracked during the delivery process and subsequent usage may be used. Watermarking and fingerprinting are two techniques that usually are employed for content marking. The DRM modules in the system also transport, store and generate, in a secure way, cryptographic keys for use in the digital content ordering and distribution process. The keys are employed for cryptographically protecting messages, including the actual digital content, during the delivery over the network.

The DRM modules also perform usage rule management and enforcement. The ordered digital content is associated with a license or digital permit specifying the client's usage rules and rights of the obtained digital media. This form of management is about the digital content itself and deals with issues such as, who gets it, how is it delivered, how may it be used (rendered, saved, forwarded, copied, executed and/or modified), how many times may it be used, how long does the rights last, who gets paid, how much they get paid and how. Some or all of these issues are specified in the license, which may be delivered together with the digital content. In order to describe the usage rules, special languages called rights languages have been developed. Two of the most prevalent rights languages used today are Rights Markup Language (XrML) and Open Digital Rights Language (ODRL). In the client's rendering device, the DRM module is implemented to ensure that the usage, most often the rendering, follows what is described in the usage rules and to prevent repudiation of the digital content usage.

Finally, charging management generally refers to the procedure of the actual payment for usage of the digital content. Several different techniques are used, such as credit card techniques for payment over Internet or payment through a subscription.

A digital content ordering and distribution system incorporating DRM functionalities is schematically depicted in Fig. 1, which illustrates the relevant parties and their mutual relationships. The system typically includes a client having access to a network through an agreement, e.g. a subscription, with a network operator. This client-operator trust relation is usually manifested in a cryptographic relationship, i.e. sharing symmetric keys or having access to each other's public keys, if asymmetric cryptography is used. A trust relationship is also present between the network operator and the content provider, but in the form of a business agreement. This agreement could be manifested by a similar key sharing and/or key access as described for the client and network operator above. However, between the client and the content provider, an induced trust relationship is established each time the client obtains digital content from the content provider. This induced trust is manifested in a session key used for cryptographically protecting the digital content as it is transmitted to the client over the network.

In a typical content ordering and distribution process, the client firstly connects to the network operator. The operator then authenticates the client and possibly verifies that the client has a valid DRM agent for managing DRM metadata, such as usage rules, encrypted data and keys, associated with the digital content. The client chooses digital content or media and specifies some client-selectable usage rules to be valid for the media, for example rendering the media a selected number of times or during a given period of time. In the present description, digital content refers to digital data that can be downloaded or streamed over a network for usage in a client module, and thus includes for example audio, video, images, electronic books and other electronic text material as well as software.

An order is then placed to the operator, which writes and encrypts a ticket specifying the ordered content and the usage rules. The ticket is sent to the client, where the DRM agent decrypts the ticket and extracts a session key from the received ticket. The ticket can be decrypted by conventional cryptographic means, e.g. using a key of a symmetric or asymmetric key pair associated with the client and the network operator. This decryption

key is preferably the client-operator subscription key, a special DRM key associated with the DRM agent, or a key derived from these keys. The extracted session key will eventually be used for decrypting the digital media from the content provider. The client also receives a copy of the ticket encrypted with the operator-content provider agreement key (or a key derived therefrom). This ticket copy is forwarded to the content provider, where the session key is extracted. Thereafter, the content provider delivers the ordered digital content cryptographically protected by the session key to the client, either as downloaded data or streaming data. Finally, the DRM agent in the client decrypts the digital content by the previously extracted session key. The digital content can be used, e.g. rendered, in the client module or an associated device according to the usage rules. Further information regarding DRM systems and ordering and distribution of digital content can be found in [2,3].

The overall content ordering and distribution process discussed above is merely given as a simplified example for conveying a general image of such processes. In order to increase the security, more authentication and cryptographic steps may be introduced. In addition, the client should pay for the ordered content, so billing and charging steps are most often present in the ordering process. Such a charging may be performed by a subscription to the network operator, by sending the client's credit card number to the network operator or a dedicated billing institute, managing the charging of digital content, or by some other means. In addition, the network operator may provide both the network and the digital content and hence acts as both operator and provider at the same time. However, the operator then typically has a dedicated content server and a dedicated operator server, so that the parties illustrated in Fig. 1 are present although the network operator also manages the content providing services. In some applications, e.g. WAP (Wireless Application Protocol) applications, it is also possible that another client may act as a content provider. However, the usage rules are then pushed to the content-receiving client from the network operator or the content provider.

The present invention is generally directed towards preventing or deterring the client from repudiating usage of the ordered digital content according to the usage rules associated with the content or by trying to violate the rules. For example, the client may have been allowed, according to the license, to render a specific digital content twice, but disagrees with the DRM agent in the client module that two renderings actually have been performed. The present invention solves this by monitoring the usage of the digital content and logging information concerning the usage individually for each usage to be monitored. By logging or recording information of client usage, the invention has a usage repudiation deterring effect on the client, lowering the risk that clients violate usage rules of ordered digital content. The generated usage information can also be used if a disagreement between the client and the content provider (DRM agent) is present. By simply investigating the log, information about the actual number of usages performed by the client, when they were performed, the quality obtained during usage sessions (depending on what is included in the usage information) can be retrieved and used to solve any issues.

In the present invention, usage of provided digital content is directed towards methods of using the content by the client. This usage could include: rendering the content by the client, for example play audio or video, display images or text and/or print the digital content; saving the content on the client module or some other suitable media; forwarding the digital content, for example to another client or client module; making copies of the content; executing the code elements of the digital content (being in form of software) and/or modifying the digital content. In a preferred application, the usage rights or rules of the relevant methods of usage are specified in the license associated with the digital content.

In the following, the embodiments of the present invention are described with usage of digital content in the form of rendering of the content. A client module then incorporates or is associated, e.g. directly or indirectly connected, with a rendering device or player for rendering the digital content. However, as the skilled in the art understands, the

invention is not limited to rendering embodiments, but comprise any other method of usage of the content by a client, including the usage described above. In such a case, the rendering device is changed correspondingly to the relevant usage means, function or device.

A client module according to the present invention is illustrated in Fig. 2. The client module can be any form of appliance, which may order and obtain digital content over a network, for example a personal computer (PC) or a mobile unit, including mobile telephones, personal digital assistants or communicators. The module comprises means for downloading or streaming the digital content from a content provider to the module, where a rendering device or player renders the content. The rendering device could be implemented in software, hardware or a combination thereof. Preferably, the rendering device includes a media processor, which may be software-implemented, for rendering the digital content using e.g. a screen or a loudspeaker, depending on the type of digital content. The rendering device may be integrated into the mobile unit or PC, but can also be provided as a stand-alone device, directly or indirectly connected thereto.

The client module is also provided with a DRM agent for managing the DRM metadata associated with the digital content. This DRM agent is implemented for decrypting digital content obtained from the content provider using session keys and enforcing rendering according to usage rules. At least a portion of this DRM functionality may be implemented in the rendering device, where the actual content rendering is performed. This rendering device associated DRM functionality could be managing for example rule-enforcement and typically also decryption of the protected digital content prior renderings thereof.

According to the present invention, a logging agent is provided in the client module, preferably in the DRM agent, for monitoring usage, in this embodiment rendering, of the downloaded or streamed digital content. This logging agent logs usage information

concerning renderings of the digital content individually for each rendering to be monitored. The logging agent generates this usage information and sends it to storing means for storage as a log entry in a log. This usage log may be arranged locally in the client module or externally. In the former case, the log is preferably stored in such a way that it is hard for an attacker to modify the usage information in the log. This could be accomplished by storing the log in a tamper-resistant device, thereby being harder to access and modify. Another solution could be to store the log somewhere in the client module, where it is hard to locate for an attacker, and/or using a format of the log, which gives no information or clue about its content. The locally stored log may be arranged in the logging agent, in the DRM agent and/or somewhere else in the client module. However, the usage information is preferably forwarded from the logging agent in the client module to an external log provided by a trusted party. This trusted party could be the network operator, the content provider or some other party, which the client and the content provider both trust.

If the usage information is sent to an external log, the information may be forwarded as it is generated. Usage information may instead be stored temporarily in the logging agent and then forwarded intermittently to the log. The information could also be sent once all renderings associated with a digital content have been consumed, i.e. when the number of renderings specified in the usage rules have been consumed or when the allowed rendering time has elapsed. In addition, the generated usage information may be sent upon a request from the content provider and/or the network operator.

Two logs may also be used, one local log stored in the client module and one external log stored at the trusted party.

The logging agent can be implemented in the client module in software, hardware or a combination thereof. The client module may be pre-manufactured with the logging agent, or the logging agent can be downloaded over the network from e.g. the network operator and implemented in the client module, which is discussed in more detail below.

As was mentioned in the foregoing, the client module can also comprises two separate units, one unit for performing the downloading or streaming of digital content and one unit that actually renders the digital content, i.e. the rendering device. The downloading or streaming unit may e.g. be a personal computer (PC) or mobile unit that stores the received digital content in or on some suitable portable media, including floppy disks, CD-ROM disks and DVD disks. The client may then move the portable media with the digital content to the rendering device for rendering the content. It is also possible to transmit the content from the downloading or streaming unit to the rendering device, where it is received and finally rendered. Typical stand-alone rendering devices include Mp3 players, CD players, DVD players, other mobile units or PCs.

Referring to Fig. 3, the logging agent can then be implemented in the rendering device, preferably in a DRM agent of the rendering device. Then, the logging agent generates usage information concerning renderings of the digital content individually and enters the information as a log entry in a usage log. This log may be stored in the rendering device, or arranged in the downloading or streaming unit of the client module, if using a stand-alone rendering device, or externally arranged in a trusted party. In the latter cases, the usage information is sent from the rendering device to the log for storage therein.

A typical implementation of a logging agent, illustrating its including elements, is shown in Fig. 4. The logging agent comprises a generator for generating usage information concerning usage of digital content individually for each usage. This generator receives input data from the usage means, or more precisely from the DRM agent managing the usage of the digital content. From this input, the information generator creates relevant usage information, more of which below, and stores it temporarily in a cache or similar temporary memory.

The usage information may then be cryptographically protected for preventing unauthorized access thereto. An encryption engine may be arranged in the logging agent

or connected thereto for encrypting the usage information using an encryption key. The encryption key may be a shared symmetric key, a copy of which is stored at a trusted party, e.g. the network operator, content provider or some other trusted party. Alternatively, an asymmetric key pair may be used for encrypting the usage information encryption. The client module then comprises a public key of a trusted party together with a certificate on the public key. The encrypted usage information can then only be read by the trusted party using its private key for decryption of the cryptographically protected information.

An authenticator for authenticating the usage information may also be provided in the client module, e.g. in the logging agent. The authenticator may introduce an authentication tag to the usage information, which is used to identify from whom the information is derived. The tag could be a digital signature added to the information using a private signing key of an asymmetric key pair. The associated public verification key together with a certificate on the public key is stored at a trusted party. Also message authentication, e.g. using symmetric keys as above for usage information encryption, may be used to authenticate and identify the origin of the usage information.

One way to do this log authentication of the usage information is by letting the DRM agent in the client module display a request on the user interface of the client module when the usage associated with the client module has used digital content. This request urges the client to confirm that a usage has been performed. In this case, in order to avoid the situation of getting no response at all, the DRM agent may be implemented to prohibit further usage of the digital content until a response, whether positive or negative, to the authentication request is given. If a positive response is given, the usage information is authenticated and stored as a log entry in the usage log. However, a negative response, i.e. the client does not accept the usage as being successfully performed nor that usage information should be entered in the log, may initiate different activities of the DRM agent. The strategy for the DRM agent to follow could be fixed or could be specified in the license associated with the digital content. In the latter case, the

content provider has the possibility to adjust the strategy to match the content and client module properties. For example, for low value digital content, one or more extra usages could be provided directly to a negative logging authentication response, while for a high value digital content the DRM agent sends an automatic message to the content provider, for the content provider to resolve the issue. Thus, in case this strategy is part of the license, it will have to be protected from being presented to the client, as he/she then could adopt his/her response strategy accordingly. Encryption of the strategy containing part of the license could give this protection.

The key(s) used for cryptographically protecting and/or authenticating the usage information could be subscription key(s) associated with the subscription between the client and the network operator, or key(s) derived therefrom. For example, the client may have a network subscription identification module, issued by the network operator, arranged in the client module. This network subscription identification module in turn comprises a key used for authenticating the client to the operator. Such a subscription key could also be used for cryptographic protection and/or authentication of usage information. Specific keys associated with the DRM agent in the client module and used in the DRM system can also be used for encryption and/or authentication purposes regarding the usage information. Also, subscription associated usernames and passwords may be used in this context. If the client has one, or several IP addresses associated thereto, such address(es) can be used for information authentication.

The generated and possibly encrypted and/or authenticated usage information is then sent from a temporary cache memory either to a log stored in the client module or through a forwarder adapted for forwarding usage information to an external log at a trusted party.

Fig. 5 illustrates a log and examples of usage information that can be found in a log entry. As was mentioned in the foregoing, the log is stored either locally in the client module and/or externally at a trusted party in some storage means or memory. If stored at a trusted party, each log may be associated with a specific client, containing only usage

information from that client. It may, however, be possible to store usage information from several different clients in one log. The information then preferably comprise some form of authentication code, identifying from which client the information is derived, more of which below.

The log entries in the log comprise usage information associated with usage, e.g. renderings, of digital content by a client module. The usage information may include a representation or description of the used digital content, e.g. a fingerprint identifying the content or the file name associated with the content. Typically fingerprints could be the content itself, a copy or portion thereof. Also hash function of the digital content or a portion thereof can be used to get a content representation. Another possible content representation is a Universal Resource Identifier (URI), which specifies the address (and possible the name of the content) of the digital content, e.g. the address in the content provider's server, from which the content can be fetched.

The usage information could also comprise information concerning the quality of the content or usage of the content. This form of information can be used to check if the usage has been performed according to the usage quality specified in the usage rules of the license, i.e. the usage should have the quality the client actually has paid for. Different quantities can be used to define and express rendering quality. Typical examples are the bandwidth or the resolution of the digital content. Also the sample rate of the digital content, if delivered as streaming data, can be used as a quality quantity. The digital content itself, or a representation thereof, could also constitute a quality quantity. For example, if the client orders and receives digital content specifying the share price of a company, for the purpose of subscribing stocks in that company, it is very important that the received content (share price) is correct and updated. In such a case, the content, or a representation thereof, can be included as usage quality in the usage information. If the client subsequently claims that he/she has received an incorrect share price, the content provider can simply retrieve the share price, obtained by the client, from the log.

Also information about usage quantity may be entered in the usage information. Such quantity could specify how many usages of the digital content that have been performed by the client, which methods of usage have been performed, and/or how many usages remain according to the usage rules.

The usage information preferably comprises information about the usage time. Such a time preferably specifies the time when the usage is completed, but could also or instead specify the start time of the usage or some other time, during which the usage is ongoing. In particular for rendering applications, but also for other methods of usage, the total time that the usage (rendering) has carried on or proceeded could constitute valuable usage information and can therefore be entered in the log. This total usage time is easily measured or estimated using the DRM agent, enabling usage of the digital content in the client module.

As was mentioned above, the usage information preferably includes some form of client authentication, identifying the client, especially when the log is stored externally. This authentication may be an authentication tag, e.g. a digital signature or message authentication, signed by the client specific key discussed in connection to Fig. 4. Instead of using a dedicated authentication tag, the whole usage information may be encrypted using an encryption and signing key, both cryptographically protecting and authenticating the usage information. If the log is stored locally in the client module, the need for an authentication tag or some other form of identifying information is somewhat relaxed.

In addition, the usage information according to the present invention is well adapted for use with location-based service. Such services are provided by e.g. network operators, which then also acts as content providers. Typically location-based service includes finding the nearest pub, restaurant, cinema, cash point, hospital, police station, etc. Also the current distance and/or direction to the relevant requested location could be given. In

such applications, the usage information may include a representation of the location of the client when ordering the location-based service, possibly together with the received digital content (direction, distance).

For games and other similar software digital content, the score or level obtained by the client when he/she renders the game can be included in the usage information. This may be especially important in situations where the client, according to the usage rule, is allowed to render the game a fixed number of times, but obtains one or several additional free renderings if he/she achieves a certain score or level associated with the game. This game score or level is then preferably entered in the usage log.

Furthermore, the entry in the usage log could comprise a record of information about the DRM agent implemented in the client module. Such DRM record preferably gives information that, and possible how, the DRM agent is involved in the usage of the digital content. Typical DRM relevant information could be a key associated with the DRM agent, or a key derived therefrom. From the DRM information it is then possible to control and verify that the client module really includes a correct and certified DRM agent. Thus, the usage information can provide a valuable source for continuously controlling clients' DRM agents to detect any security flaws as early as possible.

The log entries can also comprise other information concerning usage of digital content, such as specifying how the client has used the usage rights associated with the digital content and how many and which usages of the content that remains according to the usage rules.

The usage information can include all or some of the elements discussed above, or some other information associated with content usage.

The logging agent arranged in the client module could be implemented for generating usage information individually for each usage of digital content that is performed by the

client. In such a situation, each usage is monitored and information thereof is logged and can be retrieved later for resolving disagreements of the client and content provider. However, instead of monitoring and logging each usage, the logging agent could be configured to monitor and log usage information for randomly selected usages. The logging could also be performed intermittently for the usages, e.g. every second usage. The most important issue here is that monitoring and logging of usage of digital content should deter the client from repudiating usage of the content. By logging information intermittently or randomly, the client is not aware of which usage that is logged and therefore is deterred to repudiate the usage rules. If not every usage is logged, the client preferably should not be allowed to know which usage that actually is logged and which is not. In addition, the stragey used for logging usage information, for example which usage actually should be logged and/or when it should be logged, can be specified in the license associated with the received digital content.

Clients' usage information stored in logs can of course provide a high value source of information about actual usage of digital content. Such information may have a potential high value for content providers, when deciding business models, price of digital content, etc. Since usage information from several clients may be stored together in one or several logs at a trusted party, the content provider can then access the logs and use the information stored therein as a statistical information source in the provider's work.

If the digital content is provided as streaming data, the content provider is on-line, communicating with the client's rendering device during the rendering. In this "on-the-fly" rendering, the transport of the content is typically made with an unreliable protocol, such as User Datagram Protocol (UDP) [4]. Streaming data include digital content being rendered in real time as it is received over a network. The data can also, at least temporarily, have been buffered before the actual rendering takes place, which is well known to a person skilled in the art. The monitoring of renderings and logging of information thereof are in this case preferably made during the actual rendering. Thus, during rendering of digital content, the logging agent in the client module intermittently

generates information concerning the ongoing rendering. For example, the logging agent could be implemented to generate usage information every 30 seconds, every second minute or some other time interval, periodically or not. The generated usage information is then stored in a usage log, as discussed above. However, the usage information may preferably also be sent to the client provider for confirming reception and rendering of the streaming data. The content provider may be equipped with a DRM functionality that receives this client usage information and only continues to stream data if usage information is received within a predetermined period of time. Thus, the content provider could terminate the streaming flow of digital content if no information is sent from the client during the predetermined period of time.

In some streaming applications, the content provider intermittently sends transmitting reports to the client. These reports may include information of the hitherto delivered digital content. Such information may be the amount of data packages sent to the client and/or the quality of the delivered content. When the client receives these transmitting reports, he/she should respond by sending a receive report, accepting or rejecting that what is included in the information actually has been fulfilled, e.g. that the specified number of data packages actually have been received with the correct content quality. The logging agent can then be implemented to include the generated usage information in the receive reports. If no usage information is received by the content provider together with the receive reports, the streaming flow of digital content could be terminated, as in above.

In addition to, or as a compliment to, terminating the stream flow of data, the logging agent could include a notification in the usage information that the client refuses, or has not, sent the usage information together with the receive reports to the content provider.

In addition, protocols used specifically for streaming digital data, such as the Real-Time Transport Protocol (RTP) and the Secure Real-Time Transport Protocol (SRTP), typically have a report mechanism, where the receiver of streaming data, i.e. the client,

intermittently or periodically sends a receive report of the accompanying RTP protocol to the transmitter of the data, i.e. the content provider [5, 6]. The usage information generated by the logging agent can then be included in and sent together with the receive reports to the client provider. In addition, SRTP provides a general framework for cryptographically protecting the reports. This SRTP encryption could be used also for protecting the usage information as it is sent over the network. In SRTP it is also usually mandatory to authenticate the feedback reports, and this authentication could easily be extended by e.g. digital signatures for logging purposes.

In order to increase the security of the logging functionality in the client module, the logging agent may be implemented in a tamper-resistant device, see Fig. 6. Such a device makes it much harder for an attacker to access and modify the agent and thereby modify the logging agent and/or the generated usage information. Also, the usage log can be stored in the tamper-resistant device, thereby preventing easy access and modification by the client thereof. The tamper-resistant device is preferably portable and removably arranged in the client module. Such a device can then be moved between and used in connection with different client modules. In such a case, the client module preferably includes means for receiving and storing a license associated with received digital content. In addition, an appender for appending the usage log to the license is preferably arranged in the client module. This appender appends the log to the license so that when the tamper-resistant module is moved to another client module, both the license and the log accompany the device to the new client module. However, the appender preferably should leave the license unchanged except appending the log thereto.

Fig. 6 illustrates an embodiment of a client module incorporating a rendering device, a network communication unit and a tamper-resistant device. The network communication unit implements a network communication protocol stack, thus enables downloading or streaming of digital content from a content provider to the client. As for the embodiments above, the rendering device comprises a media processor for rendering digital content and, preferably, a DRM agent. Although not explicitly shown in Fig. 6,

a DRM agent is also preferably arranged in the tamper-resistant device. In such a case, the logging agent can be implemented in the DRM agent associated with the tamper-resistant device.

The client module can also be equipped with an input/output unit for, preferably, connection to a local network and/or appliance, e.g. a stand-alone rendering device. The network communication unit then principally manages reception/transmission of digital content and other data over the remote network provided by the network operator. Thus, other inports and outports than schematically illustrated in Fig. 6 could be present in the client module.

The embodiment of the client module in Fig. 6, could be a mobile unit, e.g. a mobile telephone. This offers an advantage compared to if the logging agent of the invention is arranged in a computer. This advantage is manifested in a potentially increased security against hacking, due to that the operating system platforms of computers, e.g. Windows and Linux, are much more well known by the public than corresponding platforms of mobile units, which thereby becomes harder to attack and modify. Therefore, a logging agent according to the present invention is well adapted for implementation in a mobile unit.

A particularly attractive solution is when the logging agent is implemented in a tamper-resistant device issued by a party trusted both by the client and the content provider. This trusted party could for example be the network operator, having a contractual agreement with the content provider to provide its subscribers with client modules. Such an operator provided tamper-resistant device could be a network subscriber identity module (SIM). This network SIM can be a smart card read by a card reader connected to the client module. Another solution is to use standard SIM cards used in GSM (Global System for Mobile Communications) mobile units or any other network SIM known to the art, including also UMTS (Universal Mobile Telecommunications System) SIM (USIM), WIM (Wireless Identity Module) and ISIM (Internet Multimedia Services Identity

Module). However, also other also other cards having similar functionalities as standard SIM cards, e.g. SIM cards used for banking transactions, could be provided with a logging agent according to the present invention.

Besides being harder to hack, due to being a tamper-resistant device, the SIM could also be used as a base for a charging mechanism that can be used for payment of digital content in the DRM system.

Fig. 7 illustrates a tamper-reistant device in form of a network subscription module incorporating a logging agent of the invention. The SIM of Fig. 7 is also provided with an Authentication and Key Agreement (AKA) module, comprising algorithms, e.g. the GSM A3/A8 AKA algorithms, for encrypting/decrypting data sent/received by the mobile unit and for authenticating the client in the network. These AKA algorithms typically uses a SIM specific key, e.g. the subscription key associated with the client-operator subscription, a key associated with the DRM agent implemented in the SIM, or a key derived from these keys. It is also possible to use asymmetric cryptography for authentication purposes. The algorithms of the AKA module can be used for cryptographically protecting and/or authenticating the usage information generated by the logging agent in the mobile unit. In such a case, the logging agent does not have to be equipped with usage information encryption and/or authentication means, but can use the AKA algorithms, or similar functions, already implemented on the SIM. The SIM is also provided with a conventional input/output unit that parses commands sent to the SIM and handles communication with the internal functions. Furthermore, resident GSM/UMTS/WAP applications are implemented on the SIM. For more information on SIM modules, reference is made to [7, 8]

The logging agent can be implemented in the SIM in software, hardware or a combination thereof. The client module, or the SIM, could be provided with the logging agent at or during manufacturing. Instead of using client module or SIM pre-fabricated with a logging agent, the logging agent can be downloaded, e.g. from the

network operator or content provider, and be implemented in the client module or SIM. This downloading solution is especially advantageous for implementing the logging agent on the SIM. As the SIM – mobile unit interface typically is associated with commands intended to send more or less arbitrary data to the SIM for use therein, e.g. the "ENVELOPE" command for GSM SIM cards, the code for implementing the logging agent on the SIM, e.g. as a general Java Applet application, could be sent using such commands. The applet can be given various degrees of authorization to access resident GSM/UMTS/WAP-related files, one possibility being to give it "full GSM/UMTS/WAP access". The logging agent application sent by the command is implemented in an application environment provided by an application toolkit associated with the SIM. For a GSM SIM the application environment is provided by SIM Application Toolkit (SAT), whereas the analogue of USIM is provided by UMTS SAT (USAT). Thus, the SIM application toolkit thus enables the operator to either "hardcode", or download, over the air, a logging agent application into the SIM besides the default GSM/UMTS/WAP application. If the logging agent is downloaded to the SIM application environment, it is preferred to authenticate the application (logging agent) as coming from the right operator. Thus, this gives protection against downloading "viruses" or incorrect logging agents form a malicious server. The downloaded logging application can also be encrypted, e.g. with a SIM associated key, so that the content thereof is not available outside the SIM. Further information of SAT and USAT is found in reference [9-11] and [12], respectively.

If using a tamper-resistant device or SIM card, other than standard SIM cards for mobile communication, its corresponding download commands and application environment can be used for implementing a logging agent application therein.

Using an application environment implemented solution for the logging agent, or a similar implementation solution, it is possible to upgrade the functions of the logging agent. This upgrade may e.g. concern a new storage location of the usage log, new information included in the logging entries, etc. Such upgrades are then simply

downloaded using download commands, e.g. the ENVELOPE command, associated with the client module and implemented in the client module. This is an advantageous solution if the logging agent is broken or "hacked", so that its code and/or secret keys become publicly known, e.g. on the Internet. Then, instead of changing all logging agent containing client modules or tamper-resistant devices, including network SIM cards, the logging agent can simple be updated by downloading and implementing new upgrades, e.g. new keys.

As is illustrated in Fig. 7, not only the logging agent but also the DRM agent is preferably implemented in the application environment. This means that also other DRM functions and applications can be upgraded through downloading.

The logging agent in the application environment generates the usage information and stores it in a usage log. This log could, as was discussed above, be stored externally at a trusted party, on the SIM and/or in the client module cooperating with the SIM. On the SIM of Fig. 7, the log may be arranged in the application environment, e.g. in the DRM or logging agent, somewhere else on the SIM.

Fig. 8 schematically summarizes the usage monitoring method according to the present invention. The method starts in step S1. In step S2 the client module uses, e.g. renders, saves, forwards, copies, executes and/or modifies, digital content received from a content provider of a network. Step S3 logs usage information concerning the usage of the digital content individually for each usage to be monitored. The method then ends in step S9. Fig. 9A illustrates the logging step S3 of Fig. 8 in more detail. Starting with step S4, a logging agent arranged in the client module generates information regarding the usage. In the optional step S7, the usage information is forwarded to a log and in step S8, the usage information is stored as a log entry in the log. The method is then completed. Two optional steps of the monitoring method are illustrated in the flow diagram of Fig. 9B. The generated usage information from step S4 is cryptographically protected, by encryption of the information using an encryption key in step S5. The encrypted

information may then be authenticated in step S6, thereby providing an identification from which client the information is derived. The method then continuous to step S7.

A DRM method according to the present invention is schematically illustrated in the flow diagram of Fig. 10. The method starts in step S10. Step S11 provides digital content from a content server to a client module over a network. In the client module the received digital content is used and a logging agent according to the invention generates information concerning the usage individually for each one of a set of client-usages. The generated usage information is then received and stored as a log entry in a log in step S12. The DRM method is then ended in step S13.

The embodiments described above are merely given as examples, and it should be understood that the present invention is not limited thereto. Further modifications, changes and improvements, which retain the basic underlying principles disclosed and claimed herein are within the scope and spirit of the invention.

REFERENCES

[1] A.J. Menezes, P.C. van Oorschot and S.C. Vanstone, "Handbook of Applied Cryptography", CRC Press.

[2] L. Kaati, "Cryptographic Techniques and Encodings for Digital Rights Management", Master's Thesis in Computer Science, Department of Numerical Analysis and Computer Science, Royal Institute of Technology, Stockholm University, 2001.

[3] Swedish patent application No. 0101295-4 filed April, 2001.

[4] J. Postel, "User Datagram Protocol", RFC 768, IETF, August 1980.

[5] V. Jacobson, S.L. Casner, R. Frederick and H. Schulzrinne, "RTP: A Transport Protocol for Real-Time Applications", RFC 1889, IETF, November 2001.

[6] M. Baugher, R. Blom, E. Carrara, D. McGrew, M. Näslund, K. Norrman and D. Oran "The Secure Real Time Transport Protocol", draft-ietf-avt-srtp-05.txt, IETF, June 2002.

[7] "Subscriber Identity Modules (SIM), Functional Characteristics", ETSI TS 100 922, GSM 02.17, Technical Specification Digital Cellular Telecommunications system, Version 3.2.0, February 1992.

[8] "Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface" 3GPP TS 11.11, ETSI TS 100 977, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, Version 8.5.0, 1999.

[9] "GSM API for SIM toolkit, Stage 2", 3GGP TS 03.19, ETSI TS 101 476, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, Version 8.4.0, 1999.

[10] "Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface", 3GGP TS 11.14, ETSI TS 101 267, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, Version 8.10.0, 1999.

[11] "Security Mechanism for SIM Application Toolkit, Stage 2", 3GGP TS 03.48, ETSI TS 101 181, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, Version 8.8.0, 1999.

[12] "USIM Application Toolkit (USAT)", 3GGP TS 31.111, ETSI TS 131 111, Technical Specification 3rd Generation Partnership Project, Technical Specification Group Terminals, Version 4.4.0, Release 4.

CLAIMS

1. A method of monitoring client-usage of digital content provided by a content provider to a client module over a network, said method including the step of:

- logging usage information concerning the usage of said digital content individually for each usage to be monitored.

2. The method according to claim 1, wherein said usage of said digital content is defined as at least one of the items in the list of:

- rendering said digital content;
- saving said digital content;
- forwarding said digital content;
- copying said digital content;
- executing said digital content; and
- modifying said digital content.

3. The method according to claim 1, wherein said logging step in turn includes the steps of:

- generating said usage information; and
- storing said usage information as a log entry in a usage log.

4. The method according to claim 1, further including the step of:

- cryptographically protecting said usage information by a protected key.

5. The method according to claim 1, further including the step of:

- performing authentication of said usage information.

6. The method according to claim 4, wherein said key is selected from the list of:

- a public key, where an associated private decryption key is stored at a

trusted party; or

- a symmetric key common to said client module and a trusted party.

7. The method according to claim 5, wherein said authentication is performed by a private key and an associated public decryption key is stored at a trusted party.

8. The method according to claim 5, wherein said authentication is performed by a symmetric key common to said client module and a trusted party.

9. The method according to claim 5, wherein said authentication is performed according to an authentication strategy specified in a license associated with said digital content.

10. The method according to claim 1, wherein said usage information comprises at least one of the items in the list of:

- a representation of said client-used digital content;
- usage quality information;
- time of usage of said digital content; and
- authentication element, identifying said client module.

11. The method according to claim 10, wherein said representation is a fingerprint of said digital content.

12. The method according to claim 10, wherein said quality information includes at least one of the items of the list of:

- bandwidth of said used digital content;
- sample rate of streaming said digital content; and
- resolution of said used digital content.

13. The method according to claim 1, further including the step of:

- forwarding said usage information from said client module to an external trusted party.

14. The method according to claim 1, wherein said digital content is used by means of a usage device in said client module, and said step of logging usage information is performed by a logging agent associated with said usage device.

15. The method according to claim 14, wherein said logging agent performs said logging step according a logging strategy specified in a license associated with said digital content.

16. The method according to claim 14, wherein said logging agent is a remotely upgradable agent.

17. The method according to claim 14, wherein said logging agent is implemented in a tamper-resistant module.

18. The method according to claim 17, wherein said usage information is stored in said tamper-resistant module.

19. The method according to claim 17, wherein said tamper-resistant module is a network subscriber identity module.

20. The method according to claim 19, wherein said logging agent is at least partly implemented as an application in an application environment provided by an application toolkit associated with said network subscriber identity module.

21. The method according to claim 20, wherein said logging agent application is downloaded into said subscriber identity module from a network operator associated

with said subscriber identity module.

22. The method according to claim 1, wherein said digital content is provided as streaming data over a network interconnecting the content provider and said client module and said digital data is rendered by said client module, and said step of logging usage information includes the step of:

- for each on-going client-rendering of streaming data, intermittently logging usage information at several occasions.

23. The method according to claim 22, further including the step of:

- intermittently forwarding said intermittently logged usage information to said content provider for confirming reception and rendering of the data.

24. The method according to claim 23, wherein said content provider terminates the flow of streaming data to said client module if no usage information has been received during a predetermined period of time.

24. The method according to claim 23, wherein said usage information is included into receive reports associated with the report mechanism of the streaming protocol used for streaming said data.

26. The method according to claim 25, wherein said streaming protocol is the Secure Real-Time Transport Protocol (SRTP).

27. The method according to claim 1, further including the steps of:

- receiving and storing a license from said content provider, said license specifying the usage rights of said digital content; and
- appending said log to said license.

28. Client module capable of using digital content provided by a content provider over a network, said content-using client module including:

- logging agent for logging usage information concerning the usage of said digital content individually for each one of a set of client-usages.

29. The client module according to claim 28, wherein said logging agent in turn includes:

- means for generating said usage information; and
- means for storing said usage information as a log entry in a usage log.

30. The client module according to claim 28, wherein said logging agent further includes:

- means for forwarding said usage information to storage means of a trusted party for storage therein as a log entry in a usage log.

31. The client module according to claim 28, further including:

- usage device adapted for using said provided digital content; and
- digital rights management (DRM) module, at least partly implemented in said usage device, having functionality for enabling usage of said digital content.

32. The client module according to claim 31, wherein said usage device in turn comprises at least one of the items in the list of:

- rendering means adapted for rendering said digital content;
- saving means adapted for saving said digital content;
- forwarding means adapted for forwarding said digital content;
- copying means adapted for copying said digital content;
- executing means adapted for executing said digital content; and
- modifying means adapted for modifying said digital content.

33. The client module according to claim 31, wherein said logging agent is implemented in said DRM module.

34. The client module according to claim 28, further including:

- means for cryptographically protecting said usage information by a protected key.

35. The client module according to claim 28, further including:

- means for performing authentication of said usage information.

36. The client module according to claim 28, further including:

- a tamper-resistant module, in which said logging agent is implemented.

37. The client module according to claim 36, wherein said usage information is stored in said tamper-resistant module.

38. The client module according to claim 36, wherein said tamper-resistant module is a network subscriber identity module.

39. The client module according to claim 38, wherein said logging agent is at least partly implemented as an application in an application environment provided by an application toolkit associated with said network subscriber identity module.

40. The client module according to claim 38, wherein said logging agent application is downloaded into said subscriber identity module from a network operator associated with said subscriber identity module.

41. The client module according to claim 28, further including:

- means for downloading upgrades of said logging agent.

42. The client module according to claim 28, further including:

- means for downloading said digital content from said content provider over a network.

43. The client module according to claim 28, wherein said digital content is provided as streaming data over a network interconnecting the content provider and said client module and said client module comprises means for rendering said streaming data, and said logging agent is configured to, for each on-going client-rendering of streaming data, intermittently generate usage information at several occasions.

44. The client module according to claim 43, further including:

- means for intermittently forwarding said intermittently generated usage information to said content provider for confirming reception and rendering of the data.

45. The client module according to claim 44, wherein said usage information is included into receive reports associated with the report mechanism of the streaming protocol used for streaming said data.

46. The client module according to claim 45, wherein said streaming protocol is the Secure Real-Time Transport Protocol (SRTP).

47. The client module according to claim 28, further including:

- means for receiving and storing a license from said content provider, said license specifying the usage rights of said digital content; and
- means for appending said log to said license, connected to said license storing means.

48. A digital rights management system including:

- means for providing digital content to a client module over a network;
- means for storing, for each one of a set of usages of said digital content by said client module, usage information concerning the usage of said digital content as a log entry in a usage log.

49. The system according to claim 48, wherein said usage of said digital content is defined as at least one of the items in the list of:

- rendering said digital content;
- saving said digital content;
- forwarding said digital content;
- copying said digital content;
- executing said digital content; and
- modifying said digital content.

50. The system according to claim 48, further including:

- means for downloading a logging agent into said client module, said logging agent being operable, when executed in said client module, for generating, for each one of said client-usages, usage information concerning the usage of said digital content and forwarding said usage information to said storing means.

51. The system according to claim 48, wherein said digital content providing means is configured for providing said digital content to said client module as streaming data, said system further including:

- means for terminating the flow of streaming data to said client module if no usage information has been received during a predetermined period of time.

52. The system according to claim 48, further including:

- means for transmitting a license to said client module, said license specifying the usage rights of said digital content.

53. The system according to claim 48, wherein said usage information is cryptographically protected by a protected encryption key, said system further including:

- means for storing a decryption key associated with said encryption key; and
- means adapted for decrypting said encrypted usage information with said decryption key, connected to said key storing means.

54. The system according to claim 48, wherein said log is stored at a trusted party providing said storing means.

55. A method of managing digital rights including the steps of:

- providing digital content to a client module over a network;
- storing, for each one of a set of usages of said digital content by said client module, usage information concerning the usage of said digital content as a log entry in a usage log.

56. The method according to claim 55, wherein said usage of said digital content is defined as at least one of the items in the list of:

- rendering said digital content;
- saving said digital content;
- forwarding said digital content;
- copying said digital content; and
- modifying said digital content.

57. The method according to claim 55, further including the step of:

- downloading a logging agent into said client module, said logging agent being operable, when executed in said client module, for generating, for each one of said client-usages, usage information concerning the usage of said digital content and forwarding said usage information for storage in said log.

58. The method according to claim 55, wherein said digital content to said client module as streaming data, said method further including the step of:

- terminating the flow of streaming data to said client module if no usage information has been received during a predetermined period of time.

59. The method according to claim 55, further including the step of:

- transmitting a license to said client module, said license specifying the usage rights of said digital content.

60. The method according to claim 55, wherein said usage information is cryptographically protected by a protected encryption key, said method further including the steps of:

- storing a decryption key associated with said encryption key; and
- decrypting for decrypting said encrypted usage information with said decryption key.

61. The method according to claim 55, wherein said log is stored at a trusted party.

62. A tamper-resistant device adapted for cooperation with a client module capable of using digital content provided by a content provider, said tamper-resistant device including:

- logging agent for logging usage information concerning the usage of said digital content individually for each one of a set of client-usages.

63. The device according to claim 62, wherein said usage of said digital content is defined as at least one of the items in the list of:

- rendering said digital content;
- saving said digital content;

40

- forwarding said digital content;
- copying said digital content;
- executing said digital content; and
- modifying said digital content.

64. The device according to claim 62, wherein said logging agent in turn includes:

- means for generating said usage information; and
- means for storing said usage information as a log entry in a usage log.

65. The device according to claim 62, wherein said logging agent further includes:

- means for forwarding said usage information to storage means of a trusted party for storage therein as a log entry in a usage log.

66. The device according to claim 62, further including:

- means for cryptographically protecting said usage information by a protected key.

67. The device according to claim 62, further including:

- means for performing authentication of said usage information.

68. The device according to claim 62, further including:

- means for downloading upgrades of said logging agent.

69. The device according to claim 62, wherein said tamper-resistant device is a network subscriber identity module.

70. The device according to claim 69, wherein said logging agent is at least partly implemented as an application in an application environment provided by an

application toolkit associated with said network subscriber identity module.

71. The device according to claim 70, wherein said logging agent application is downloaded into said subscriber identity module from a network operator associated with said subscriber identity module.

72. The device according to claim 62, further including:

- means for receiving and storing a license from said content provider, said license specifying the usage rights of said digital content;
- means for appending said log to said license, connected to said license storing means.

ABSTRACT

The invention refers to methods, equipment and systems used to monitor usage of digital content provided from a content provider over a network to a client module. In the client module, a logging agent generates and stores information concerning usage of the digital content individually for each usage to be monitored. The generated information is entered in a usage log, either stored in the client module or at a trusted party. The entries of the log may include a representation of the content, information about usage quality, usage time and/or authentication tag, identifying the client. The usage information is preferably cryptographically protected. The logging agent is preferably implemented in a portable tamper-resistant module, e.g. a network subscription identity module. The module may be pre-manufactured with the logging agent, or the agent can be downloaded thereto. The agent is preferably upgradable by downloading and implementing new logging applications.

(Fig. 6)

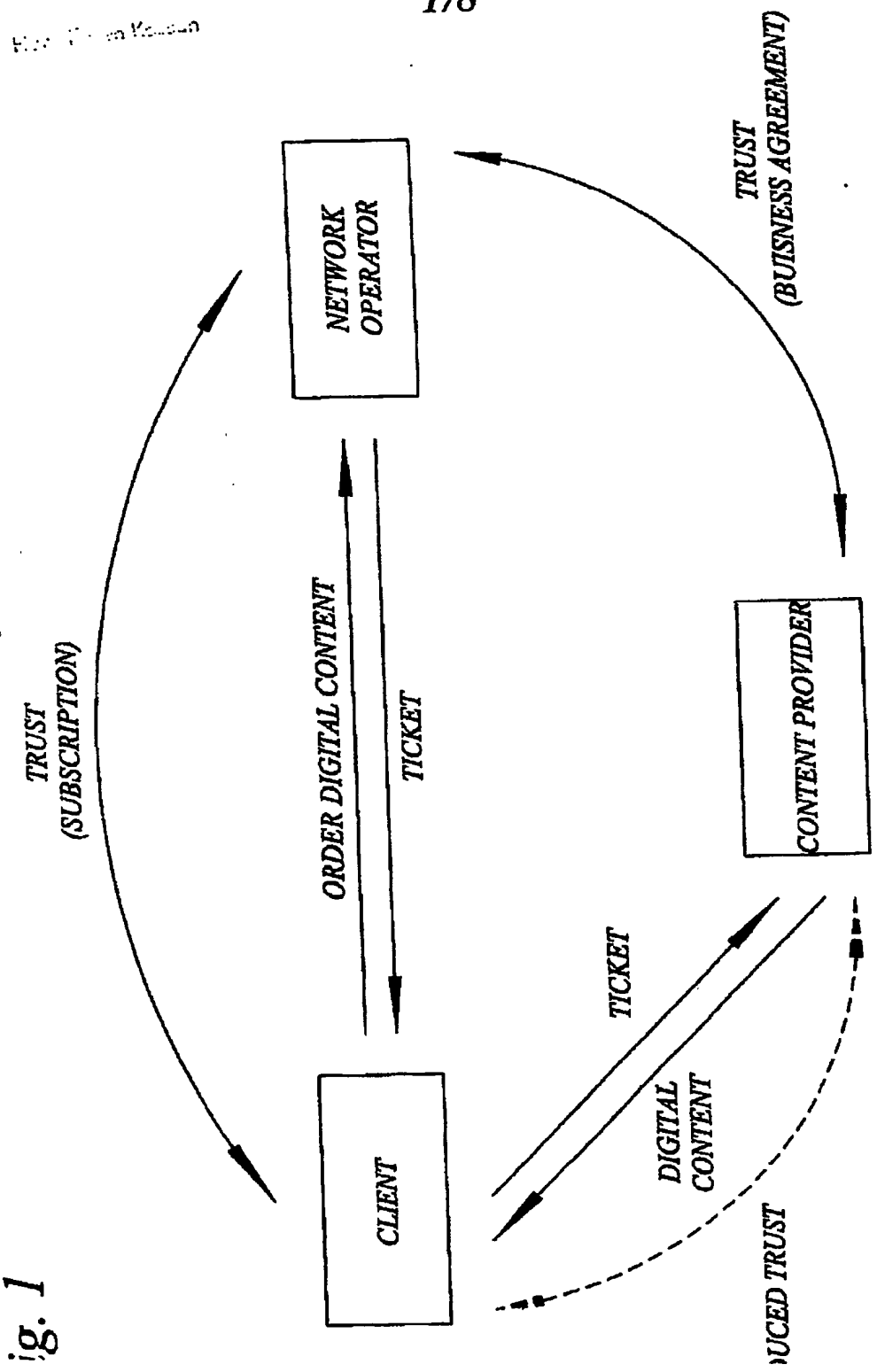

NETWORK OPERATOR
TRUST (BUISNESS AGREEMENT)
CONTENT PROVIDER
ORDER DIGITAL CONTENT
TICKET
TRUST (SUBSCRIPTION)
TICKET
DIGITAL CONTENT
CLIENT
UCED TRUST

Fig. 1

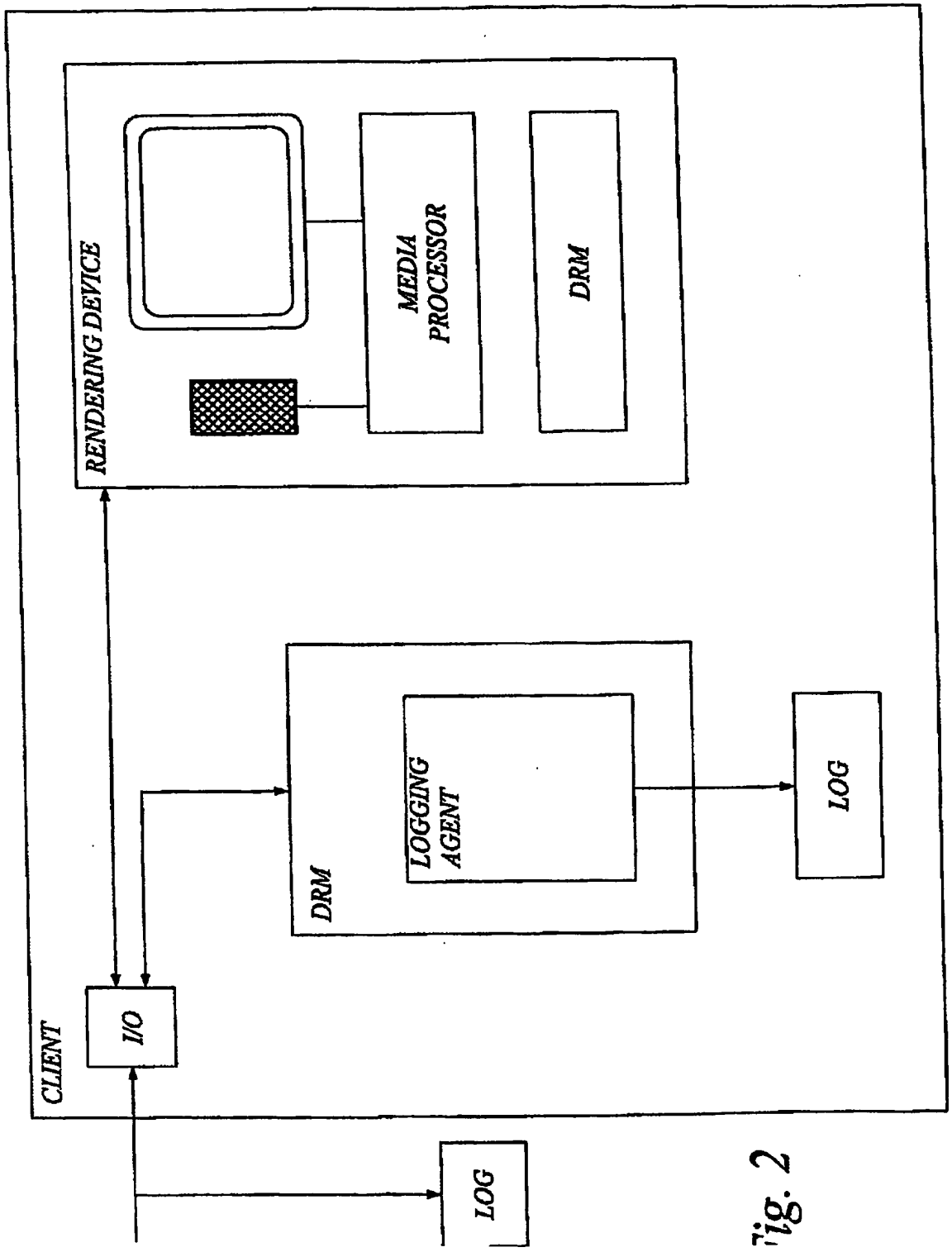

RENDERING DEVICE
MEDIA PROCESSOR
DRM
DRM
LOGGING AGENT
LOG
CLIENT
I/O
LOG

Fig. 2

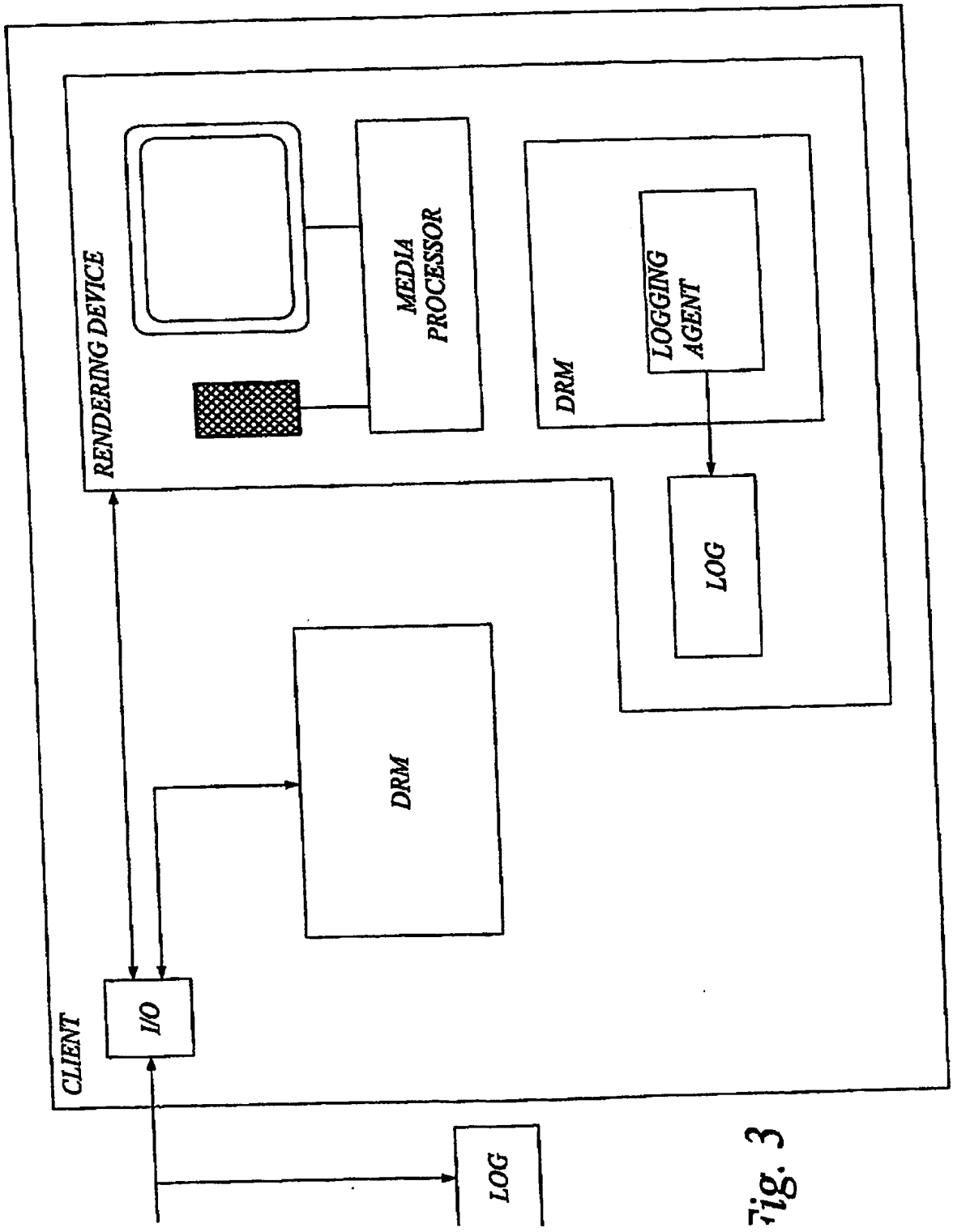

RENDERING DEVICE
MEDIA PROCESSOR
DRM
LOGGING AGENT
LOG
DRM
CLIENT
I/O
LOG

Fig. 3

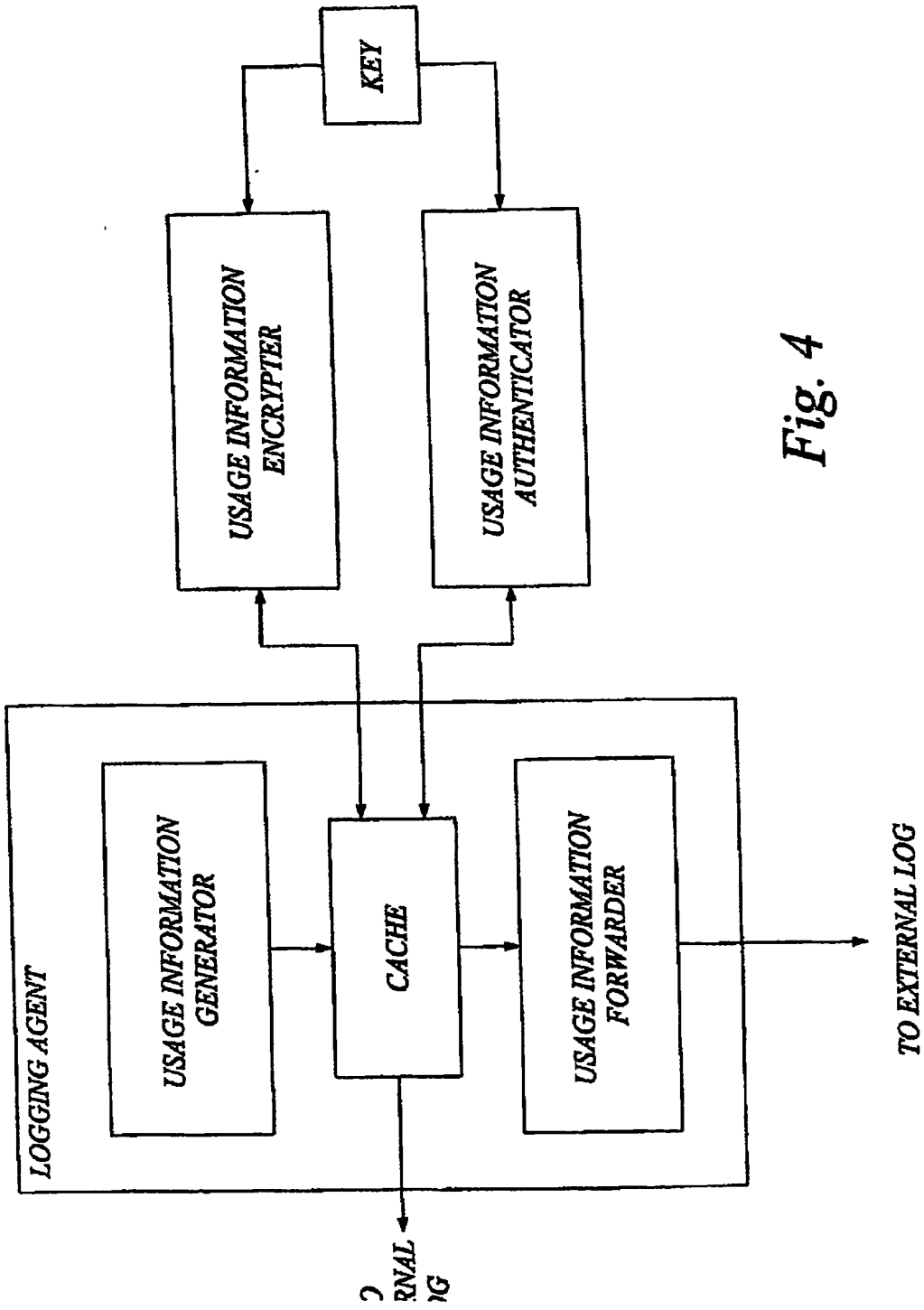
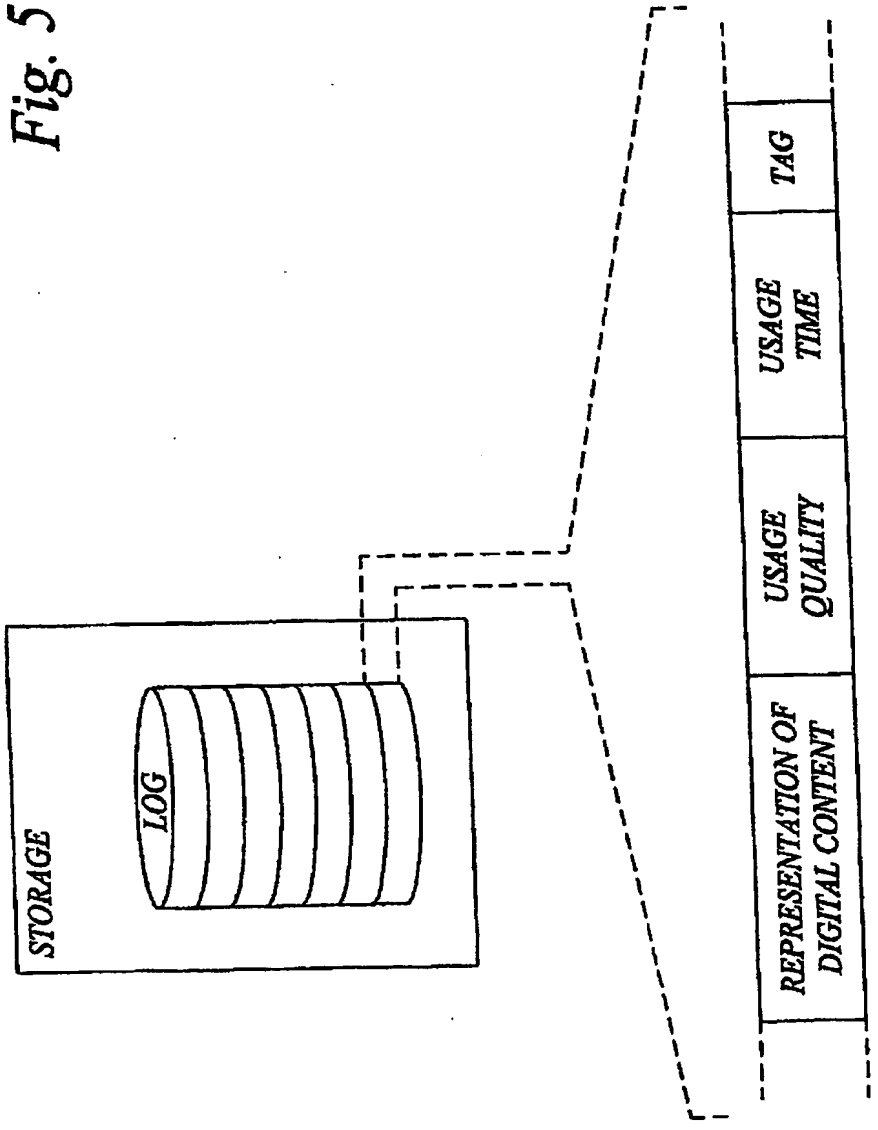

KEY
USAGE INFORMATION ENCRYPTER
USAGE INFORMATION AUTHENTICATOR
LOGGING AGENT
USAGE INFORMATION GENERATOR
CACHE
USAGE INFORMATION FORWARDER
TO EXTERNAL LOG

Fig. 4

Fig. 5


STORAGE
LOG
REPRESENTATION OF DIGITAL CONTENT
USAGE QUALITY
USAGE TIME
TAG

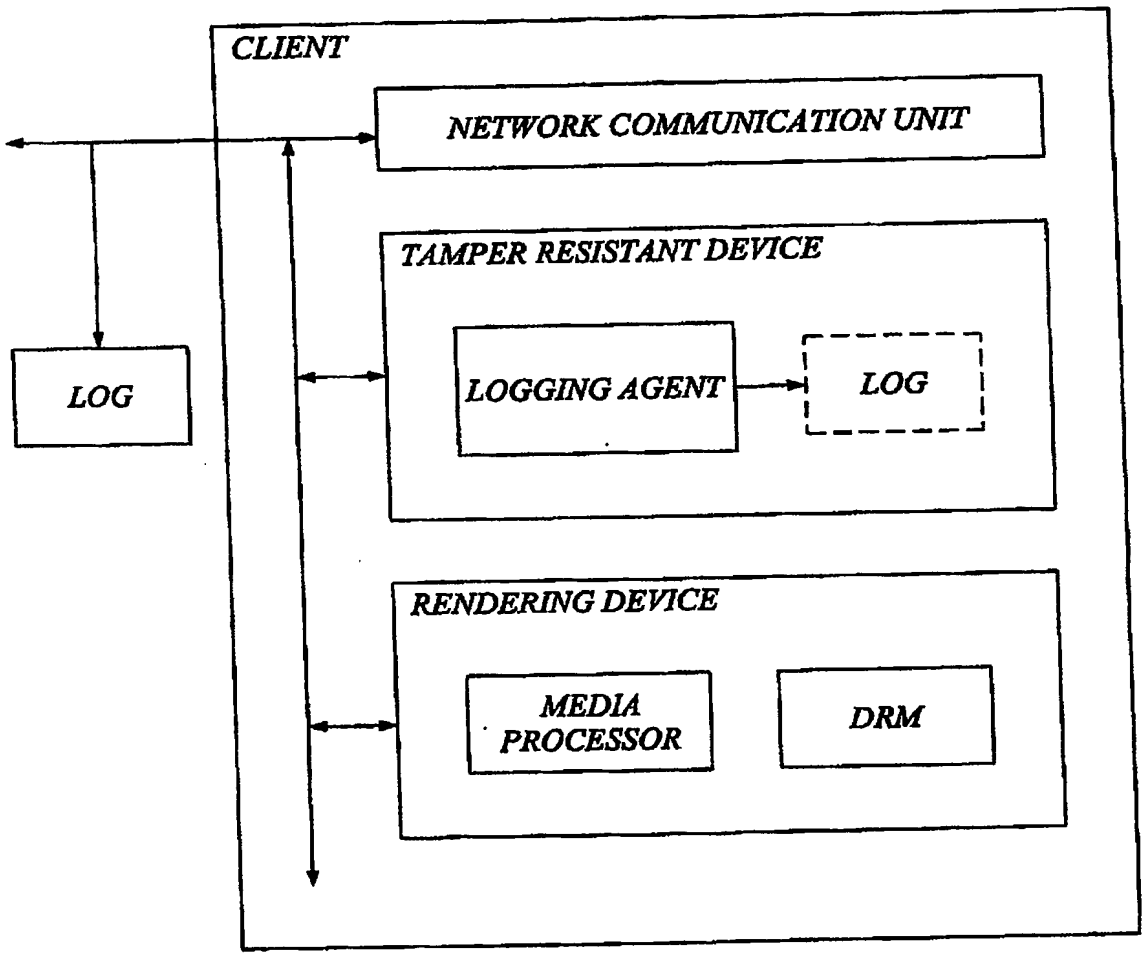

CLIENT
NETWORK COMMUNICATION UNIT
TAMPER RESISTANT DEVICE
LOGGING AGENT
LOG
LOG
RENDERING DEVICE
MEDIA PROCESSOR
DRM

Fig. 6

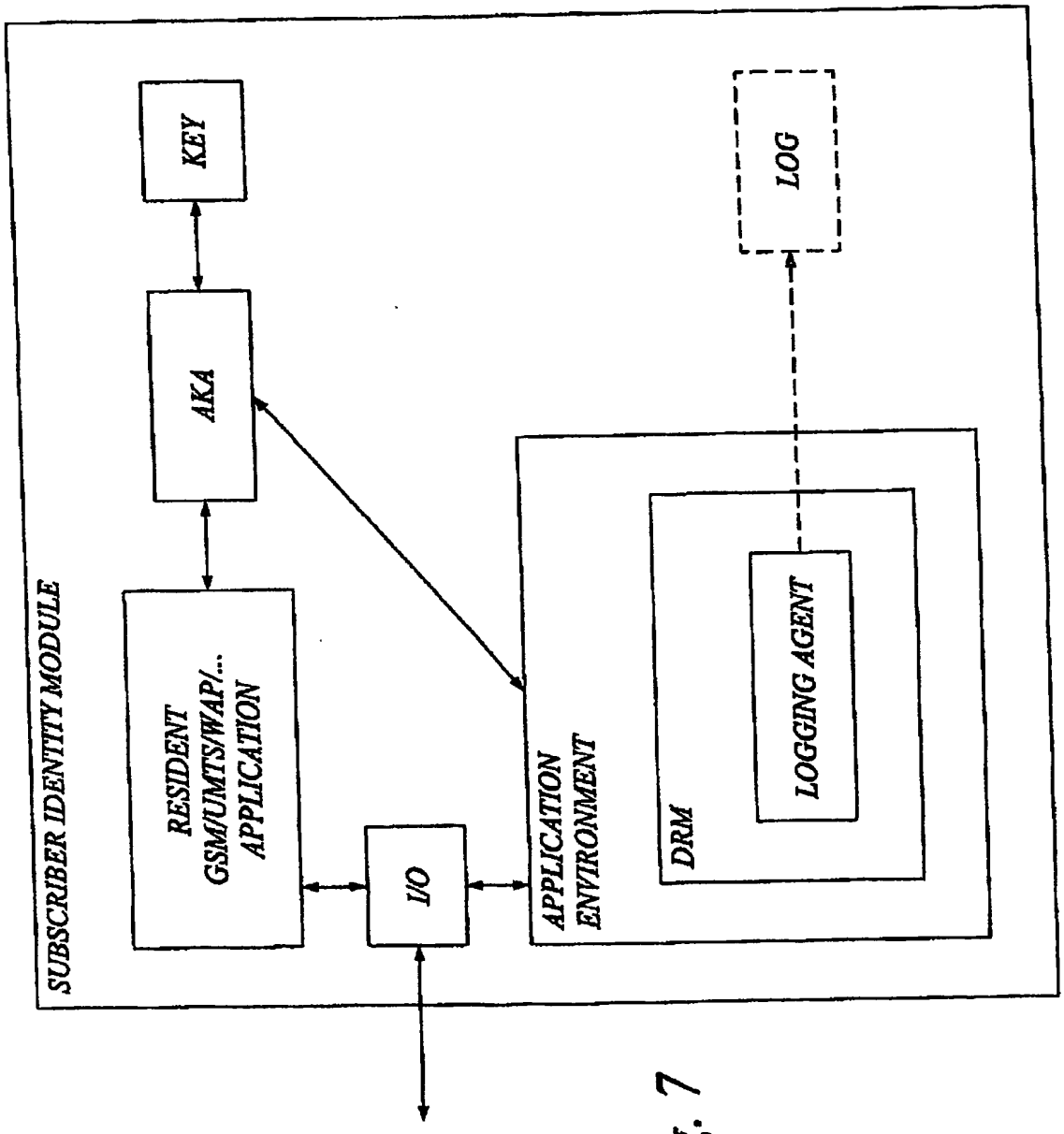

SUBSCRIBER IDENTITY MODULE
KEY
AKA
RESIDENT GSM/UMTS/WAP/... APPLICATION
I/O
APPLICATION ENVIRONMENT
DRM
LOGGING AGENT
LOG

Fig. 7

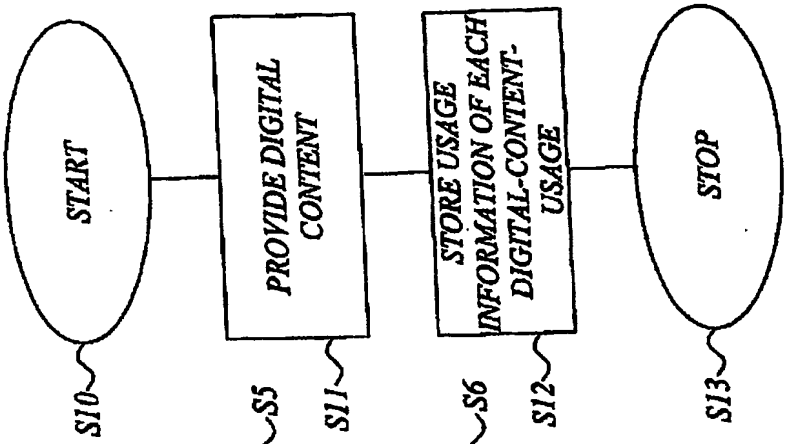


Fig. 10

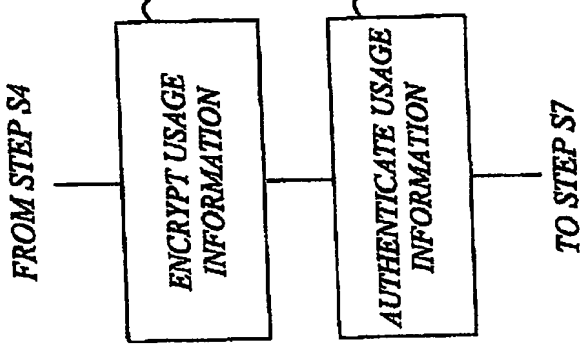


Fig. 9B

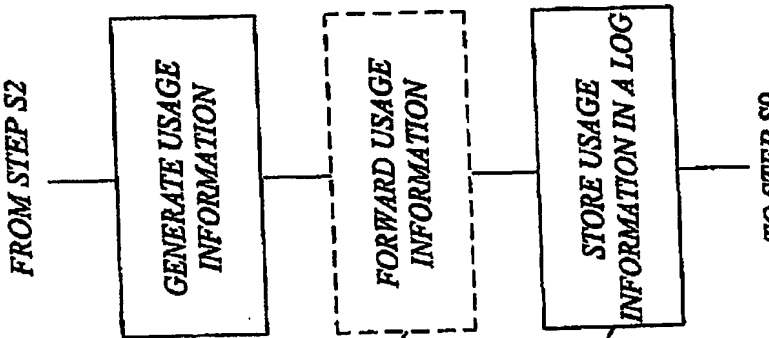


Fig. 9A

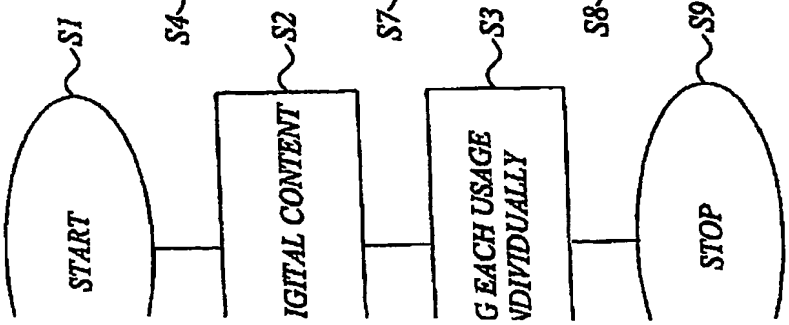


Fig. 8

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.